IntelCrawler

Intelligence Report

Lizard Squad / Guardian of Peace (GOP)

FOR PUBLIC RELEASE




Century Plaza Towers, 2029 Century Park East, Suite 400, Los Angeles, P: (424) 202 3604, info@intelcrawler.com (PGP)

Intelligence Request

Description	
INT-REQ-ID	INT-REQ-451
Background	"Lizard Squad" is a group of hackers, responsible for DDoS attacks against: - EA Games; - Xbox Live; - Sony Playstation Network; - RockStar Games. "GOP" is a group of hackers, responsible for cyber attack against Sony. Analysis shows some linkage and correlation between "Lizard Squad" and so-called "GOP". The details in the report may help attribution and some IOA's may help defend future attacks.
Priority	High
Target Date	Report Immediately When Available

Table of Contents

Intelligence Request **2**

Table of Contents **3**

Adversary Profiles **4**
Lizard Squad 4
"abdilo" 4
"lolaristocrat" 9

Chronological Analysis **12**
August 24th 2014 12
August 26th 2014 12
November 21th 2014 13
November 24th 2014 13
November 26th 2014 15
December 1st 2014 – "I am the boss of G.O.P." 15
December 3st 2014 – "We have released the data of Sony Pictures here" 16
December 5st 2014 – "I am the head of GOP" 16
December 6th 2014 – "Gift of GOP for 2nd day" 16
December 7th 2014 – "Gift of GOP for 3rd day Financial data of Sony Pictures" ..17
December 8th 2014 – "Gift of GOP for 4th day" 17
December 10th 2014 – "Gift of Sony for 5th day: My Life At The Company-Part 1"18
December 11th 2014 - "Gift of Sony for 5th day: My Life At The Company-Part 2"18
December 14th 2014 - "The sooner SPE accept our demands, the better" 18
December 18th 2014 - "Dear Sony from GOP" 19
December 19th 2014 - "Message to CEO of Sony – Michael Lynton" 20
December 20th 2014 - "Christmas gift to FBI" 22
December 22th 2014 - "Working together with GOP on a Christmas project" 22
December 29th 2014 - "Well, we do know some people from the GOP" 25
December 30th 2014 - "Looking at this south korean powerplant" 25
December 31th 2014 - "Suicide Hacking in Australia" 26
A.1 28
January 3d 2015 - "GOP: Final message to Sony and world" 31
Appendix A. - Lizard Squad / GOP Characteristics 32
Appendix B. – Social Graph 34
Conclusion 35

Disclaimer **36**

Adversary Profiles

Lizard Squad

Lizard Squad is a group of cybercriminals, having 8 key members – "dragon", "komodo", "ryan" (was arrested), "sp3c", "adbilo", "chameleon", "vagineer" or "vinnie" (was arrested), & "gecko". This group started to position themselves as Hacktivists, attacking big corporations, primarily gaming servers. There are also several other bad actors which appeared after the first cyber attacks of the group, such as "ice", "MLT", "alg0d", "jordie" (was arrested), "teridax" and "lolaristocrat", who allegedly acted as one of the main operators on their IRC channel.

The group has several technical leaders, as well as some ideological support, having no ties to cyber attacks or practical hacking. One of the first cyber attacks on behalf of the group was performed against the Sony Playstation Network, and several other corporations. Since these first attacks, the profile of the group has significantly changed.

Some of their key members, such as "Abdilo" and "lolaristocrat" have become more independent, performing cyber attacks against military, government and private sector network resources without any clear motivation. There are several identified Twitter accounts with the hashtag #KimJongSec, created by the last bad actor for reasons unknown. The account promotes DDoS attacks against South Korea and their President's WEB-site.

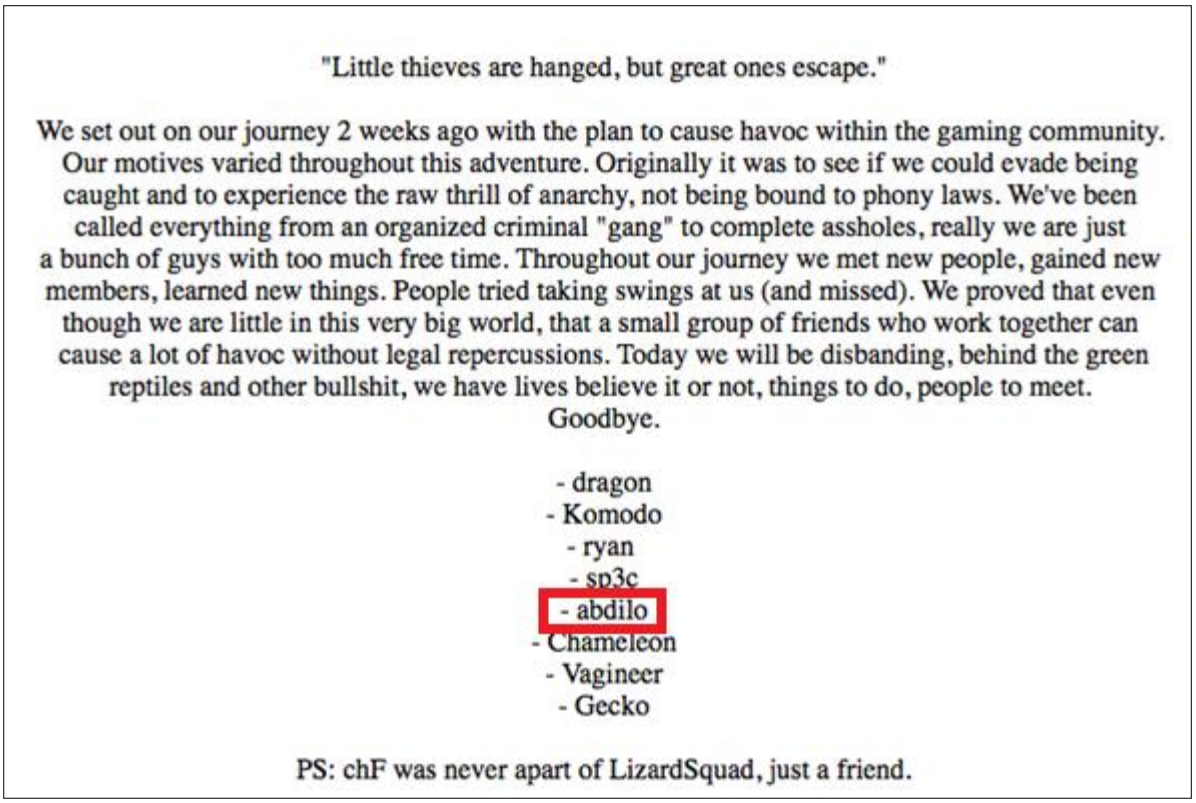
As of October 2014, "Abdilo" left Lizard Squad per his postings, but retained some relations with its key members. Later in December 2014, "Abdilo" also published several posts supporting North Korea, while continually showing aggression against the US and Australian Government.

He also attacked one of the biggest nuclear energy companies in South Korea - Korea Hydro & Nuclear Power (KHPN)[12], targeting their power plant infrastructure, where "non-critical" data seemed to have been stolen. Before the attacks against South Korea, "Abdilo" had compromised several government resources of the US and Australia Government.

"abdilo"

In one of the messages from Lizard Squad, a nickname of "Abdilo" appears:

[1] http://www.reuters.com/article/2014/12/22/us-southkorea-nuclear-idUSKBN0K008E20141222
[2] http://www.reuters.com/article/2014/12/30/nuclear-southkorea-cybersecurity-idUSL3N0UE1A320141230



"Little thieves are hanged, but great ones escape."

We set out on our journey 2 weeks ago with the plan to cause havoc within the gaming community. Our motives varied throughout this adventure. Originally it was to see if we could evade being caught and to experience the raw thrill of anarchy, not being bound to phony laws. We've been called everything from an organized criminal "gang" to complete assholes, really we are just a bunch of guys with too much free time. Throughout our journey we met new people, gained new members, learned new things. People tried taking swings at us (and missed). We proved that even though we are little in this very big world, that a small group of friends who work together can cause a lot of havoc without legal repercussions. Today we will be disbanding, behind the green reptiles and other bullshit, we have lives believe it or not, things to do, people to meet. Goodbye.

- dragon
- Komodo
- ryan
- sp3c
- abdilo
- Chameleon
- Vagineer
- Gecko

PS: chF was never apart of LizardSquad, just a friend.

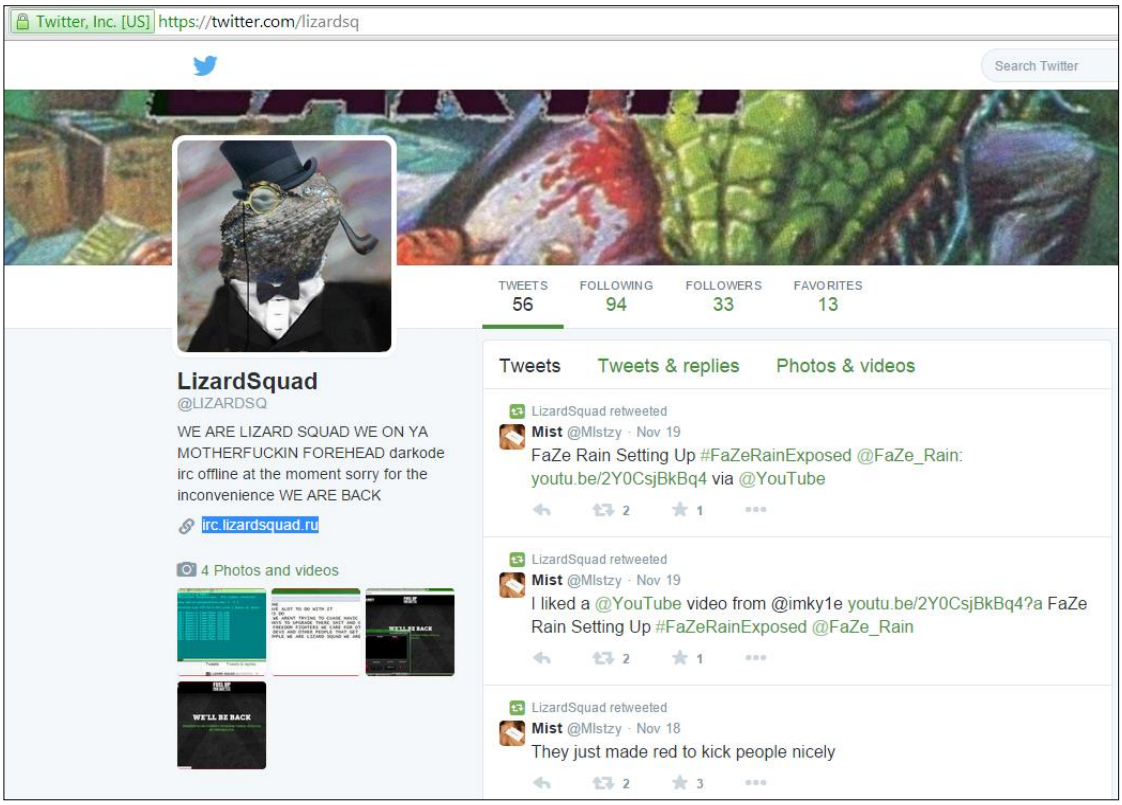
Pic.1 – The key members of Lizard Squad. This list will change later, as some members will leave the group, and new Hacktivists join the group

Using operatives and networked resources, discovery revealed that the domain name "lizardsquad.ru" was registered on the following e-mail - surivaton@gmail.com.

Later, "Abdilo" explains, that he was the owner of this domain name, but after some time, left the group.

*I joined back in august, messed around and I hosted lizardsquad.ru and lizardsquad.com. I never had control of the ddos botnet. Left lizardsquad back in october but still talk with the members. One of lizardsquad's members used one of my domain accounts to register lizardpatrol.com(thus linking one of my old emails with lizardpatrol).**(December 31st, "Abdilo")***[3]

[3] http://pastebin.com/DvSf6dAK



Pic.2 – One of the official domain names of Lizard Squad

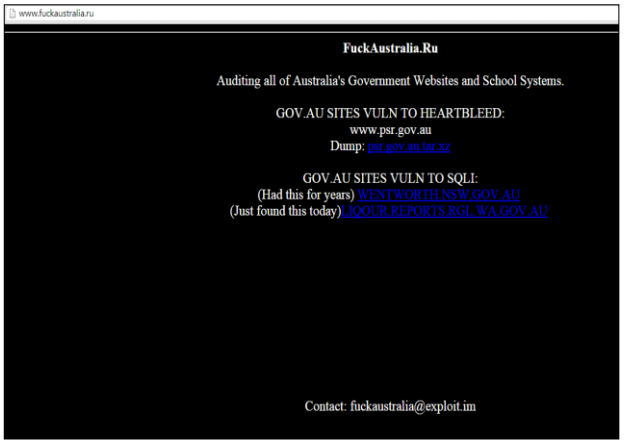
“abdilo_”	
Lastname	Crees
Firstname	David
E-Mail	surivaton@gmail.com
Accounts	Facebook https://www.facebook.com/ARMHF?fref=ts (“Root Toor”); GitHub https://github.com/surivaton (“David Crees”); YouTube https://www.youtube.com/watch?v=M7TnYo7pnkA ; Google Plus https://plus.google.com/116092303179922520941/posts ; Reddit https://www.reddit.com/user/surivaton
Location	Gladstone, Queensland, Australia Calliope, Australia
Skype	Skype: “facebook:surivaton”
Jabber	abdilo@exploit.im abdilo@darkcode.com
Nicknames	Abdilo, Notavirus, Surivaton, Grey Hat Mafias Bitch
Profiles	Hackforums: http://webcache.googleusercontent.com/search?q=cache:BYOA0DBtjPAJ:www.hackforums.net/showthread.php%3Ftid%3D4331159%26page%3D15+&cd=18&hl=en&ct=clnk&gl=ru P0wersurge.com: https://www.p0wersurge.com/forums/introductions/12879-hi/

	Exploit.in: https://exploit.in/forum/index.php?showuser=55603
Comments	Had agoraphobia during childhood WEB-applications hacking, Botnets Hacking AUtism is mentioned on one of his profiles

Table 1 – "Abdilo" Profile

Besides the identified Lizard Squad's domain name, there were other identified domain names registered by this bad actor in the past, using the same e-mail and details:

Abdilo.ru



Fuckaustralia.ru

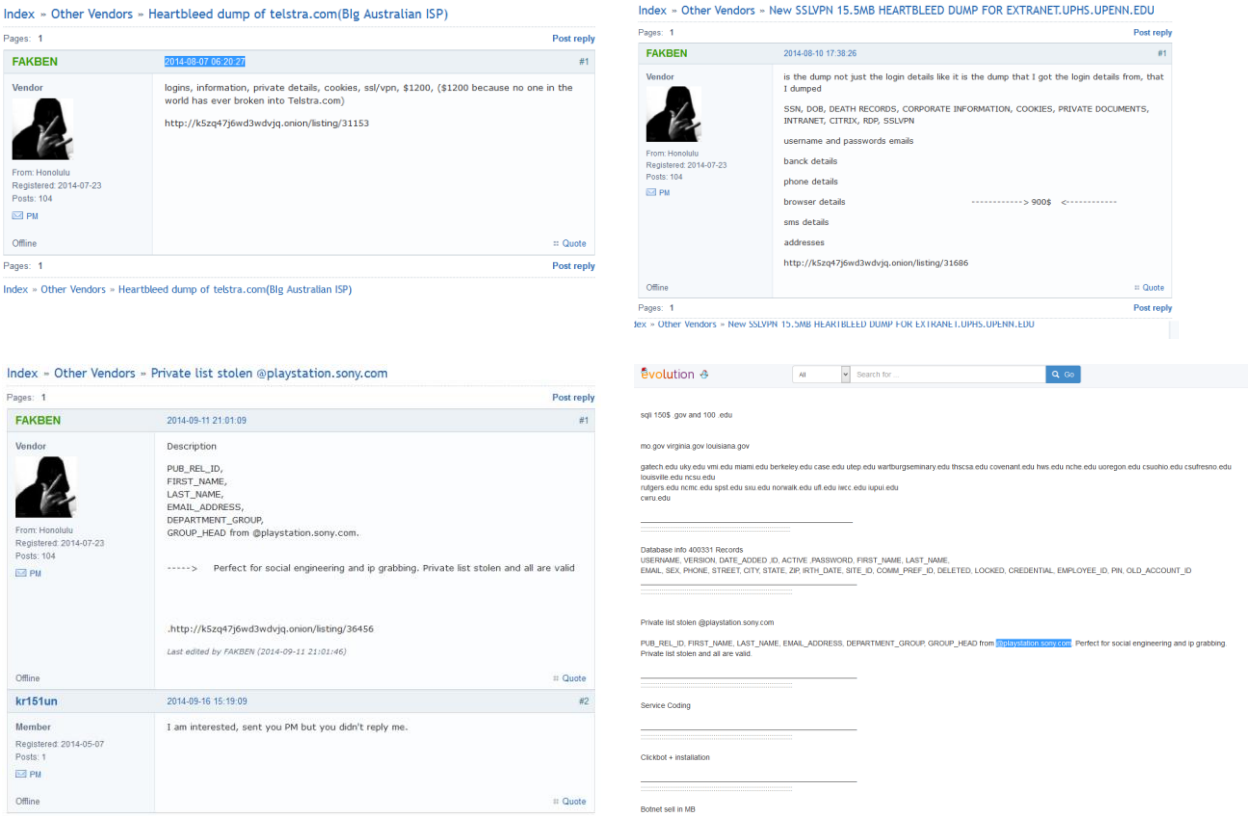
Pic.3 – Domain names, owned by "Abdilo", had Jabber contact: fuckaustralia@exploit.im and information about vulnerabilities on Australian government WEB-resources

In March 2014, the identified bad actor published information about SSL vulnerabilities[4] in Juniper devices, exposing vulnerable network resources:

- extranet.uphs.upenn.edu;
- vpn.stloiscountymn.gov;
- vpn1.broadcastaustralia.com.au;
- remote.compumenn.com.au;
- rna.n.nsa.nexus.telstra.com.au.

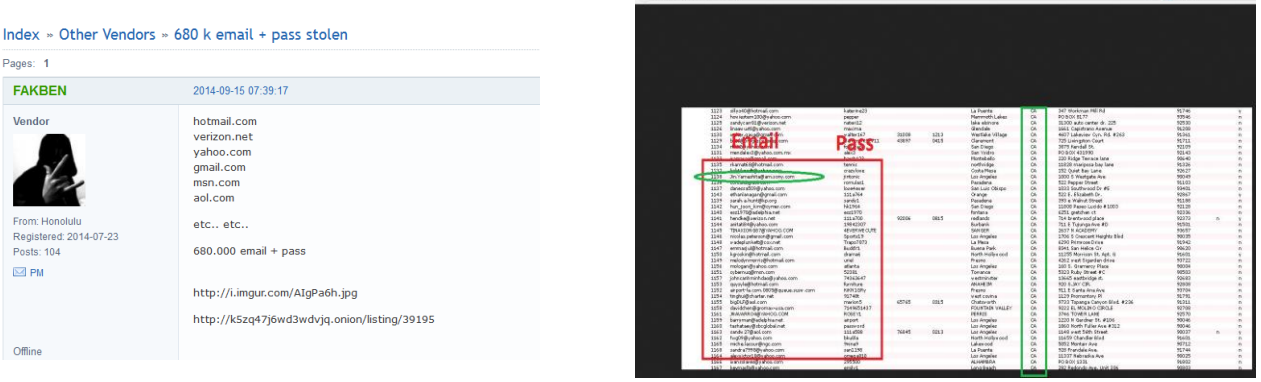
The same resources, which include "stolen lists from @playstation.sony.com", were traded on the black market by a bad actor, having the nickname "FAKBEN"[5].

[4] http://www.div-13.com/view/7c5afed3
[5] http://i25c62nvu4cgeqyz.onion/profile.php?id=9490



Pic.4 – Identified bad actor "FAKBEN", trading the same information as former Lizard Squad member "Abdilo" in the underground

The structure of the data has "DEPARTMENT_GROUP" and "GROUP_HEAD", which might be related to internal corporate information from Sony network or one of their compromised applications, which may have housed employee data.



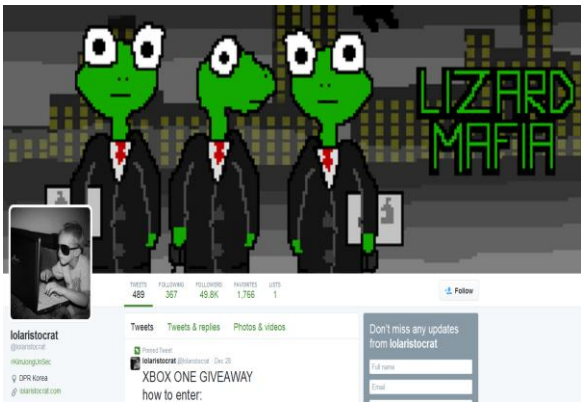
Pic.5 – The bad actor proposed lists with leaked employees data

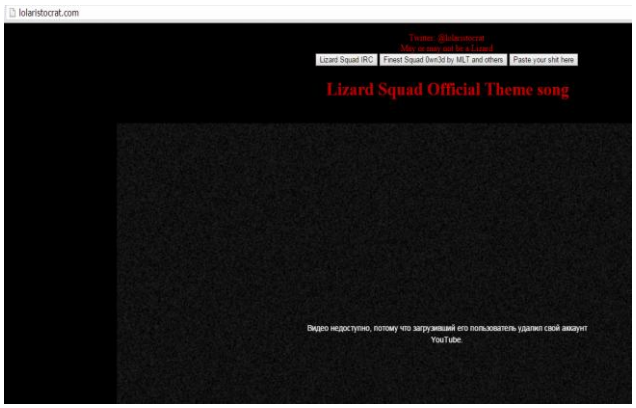
In one of the articles related to the first DDoS attacks on big e-gaming services, there was a mention of the bad actor "GOPGangster"[6], who released some details about the incident. Lizard Squad member "Abdilo", commented on the article using one of his old nicknames.

"Hundreds of people started to post about compromised accounts. One thread, from a user named GOPGangster, detailed how it happened. On Aug. 20, Jason contacted him and threatened to take over his account. "I didn't believe him until my account was taken," GOPGangster wrote. He knew he "was screwed," he said, when his friend asked him why he left his ranked team. His account then wrote "I am God, Jason," and transferred to Riot's Oceania server. The password to the account was long and included "lots of random things that would be very difficult to grab," GOP Gangster recalled. "Worst of all my account had my credit card info saved."

"lolaristocrat"

"Lolaristocrat" has referenced DPR (North Korea) in his Twitter account, clearly written in English. According to analysts, this bad actor created several Twitter accounts, some time ago.





https://twitter.com/lolaristocrat (Twitter)

http://lolaristocrat.com/ (WEB-site)

Pic.6 – Twitter and personal WEB-site of "lolaristocrat"

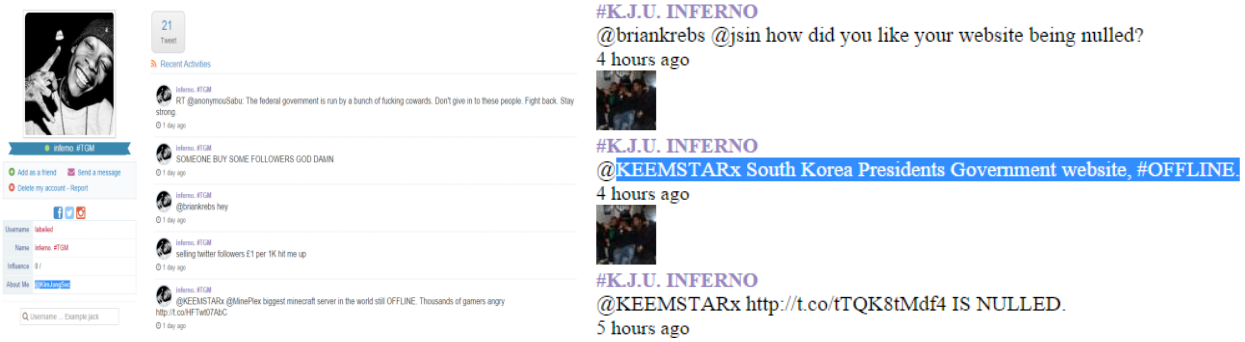
Three Twitter accounts have been identified with hashtag "#KimJongSec", followed by two Lizard Squad members – "Abdilo" and "alg0d".

[6] http://www.dailydot.com/esports/jason-shane-duffy-league-of-legends-hacks/

https://twitter.com/KimJongSec (new) https://twitter.com/PacketoPortal (old)

Pic.7 – Identified Twitter accounts with hashtag "KimJongSec" and link to Lizard Squad member "lolaristocrat"

Previously, the "KimJongSec" account had the name "K.J.U[7]. INFERNO", publishing DDoS attacks against South Korean WEB-sites, including the official site of the President.

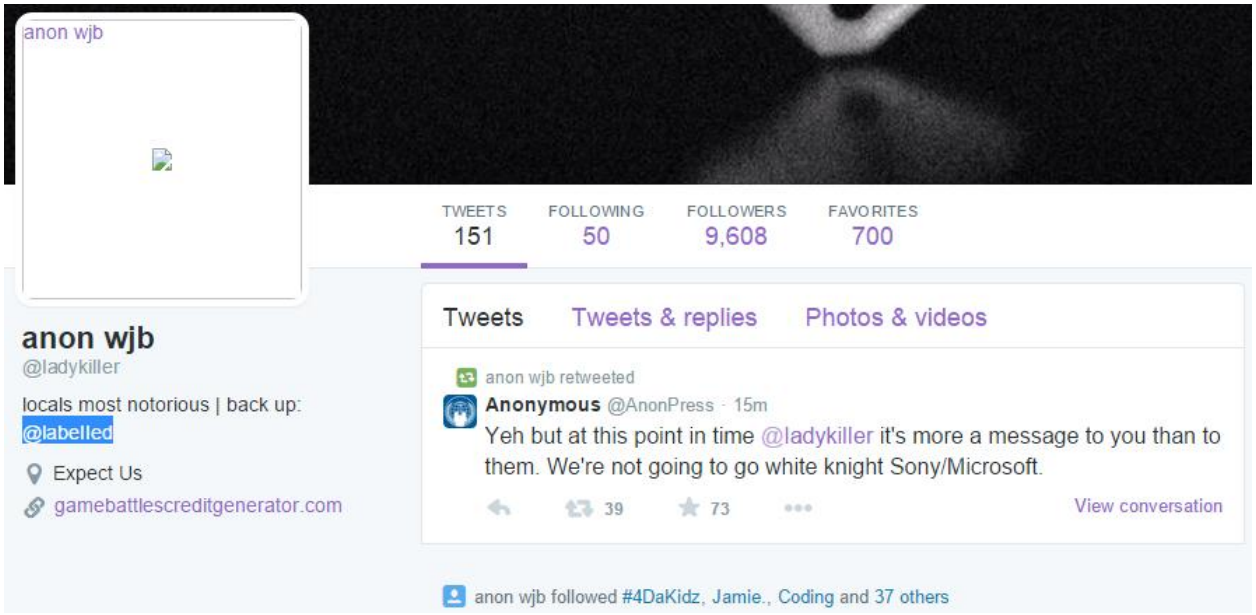


Pic.8 – Old Twitter account, maintained by user "labeiied"

[7] K.J.U – "KimJongUnSec"

The initial account belonged to Twitter with the username "labeiied"[8], which appears to be an alias to an account of the Hacktivists using nickname "labelled" ("anon wjb", "iadykiller).

I only ever DDoS when i'm high. @KimJongSec



Pic.9 – The identified account of "labelled" also contained posts about Sony

[8] http://webcache.googleusercontent.com/search?q=cache:CuzuGryNM-0J:https://www.toptweet.org/user/labeiied+&cd=6&hl=en&ct=clnk&gl=uk

Chronological Analysis

August 24th 2014

Lizard Squad published the message, directly addressed to Sony[9] (11:03 AM):

Pic.10 – Lizard Squad has threatened a Sony executive with a fake post about explosives in the plane

The same day, 1:29 PM, Lizard Squad tweeted at American Airlines saying that a flight carrying John Smedley, president of Sony Online Entertainment had "explosives on-board".

August 26th 2014

Lizard Squad performed DDoS against Sony PSN and published several messages addressed to Sony. As a defense, one of the posts contained references to monetary gain. This post demonstrates concern regarding Sony's costs for defense:

"Sony, yet another large company, but they aren't spending the waves of cash they obtain on their customers' PSN service. End the greed." — Lizard Squad (@LizardSquad) August 24, 2014

HEY @Sony PICK UP THE PHONE

— Lizard Squad (@LizardSquad) August 26, 2014

[9] http://abcnews.go.com/Technology/lizard-squad-group-claiming-responsibility-high-profile-hacks/story?id=25129458

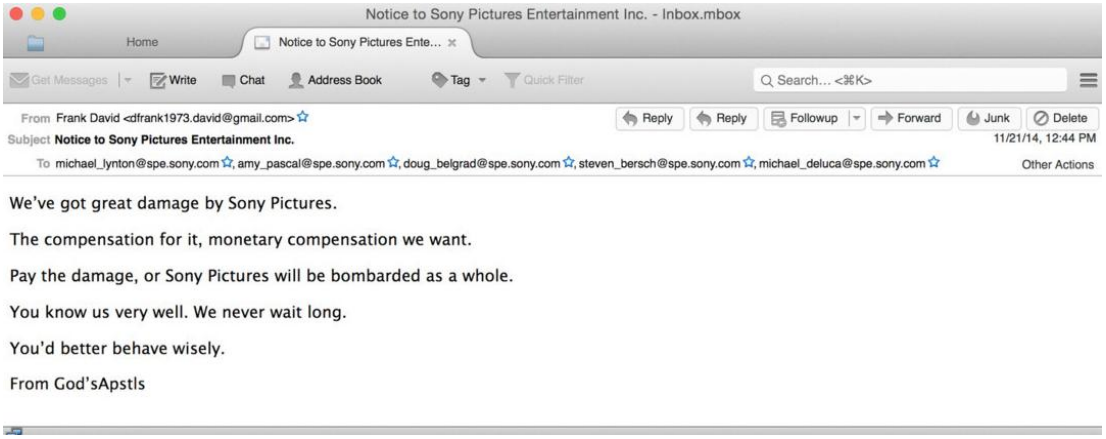
YO @Sony can we get estimates on how many $ you paid for @prolexic?

— Lizard Squad (@LizardSquad) August 26, 2014

Pic.11 – The majority of Lizard Squad posts are directly addressed to Sony

November 21th 2014

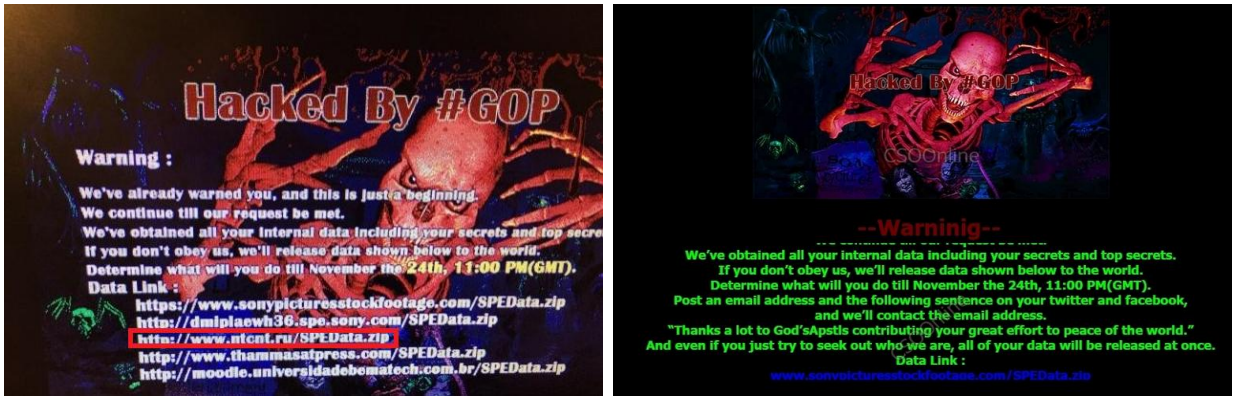
During the initial stage, GOP sent a letter to Sony, asking for monetary compensation to prevent the leak:



Pic.12 – Anonymous hackers from GOP asked for monetary compensation from Sony

November 24th 2014

GOP provided Sony with a deadline, November 24th:



Pic.13 – GOP announced a deadline for Sony

These posts did not contain any information about the film "The Interview".

Previously, the attackers posted to at least three Twitter feeds, leaving the same message: "*You, the criminals including [Sony Pictures CEO] Michael Lynton will surely go to hell. Nobody can help you.*" The image posted with the message shows a digitally edited image of Lynton's head in a dark, hellish landscape.

Pic.14 – GOP published a negative post in hacked Twitter accounts about a Sony executive

The links on the leaked files were published in social networks and uploaded on Torrents.

November 26th 2014

The GOP leader published the following message:

```
posted *DS* 10:23 PM Wednesday, November 26, 2014 Greenwich Mean Time (GMT)

cut/paste ******************************************************************

RE: To The Guardians Of Peace
From: godsapstls.boss4@unseen.is
Date: 2014-11-26 17:11
I am the head of GOP.

I appreciate you for calling us.
The data will soon get there.
You can find what we do on the following link.
https://www.facebook.com/pages/The-Guardians-Of-Peace/604245239697994

God bless us.

God's Apostles

******************************************************************************
```

Pic.15 – Anonymous hackers sent an e-mail to Sony

December 1st 2014 – "I am the boss of G.O.P."

GOP published a message about stolen data:

I am the boss of G.O.P. A few days ago, we told you the fact that we had released some of Sony Pictures Bilms including Annie, Fury and Still Alice to the web. Those can be easily obtained through internet search. For this time, we are about to release Sony Pictures data to the web. The volume of the data is under 100 Terabytes. You can get some of the data at [Links Redacted] We will release all of the data at [XXX and [XXX] in a short time(the minimal time needed for handling tens of TBs of data). The password of the document is "diespe123". Besides, we have much more interesting data than you know. If you Bind special interest, send an email in a method we have explained before. Thanks

December 3st 2014 – "We have released the data of Sony Pictures here"

GOP published the following message:

Hi, We have released the data of Sony Pictures here http://pastebin.com/zUyA0EiX And you can Bind data as it adds in PASTEBIN using tags of GOP, SONY, SPE and etc. Today more interesting data will be presented for you. Thanks

December 5st 2014 – "I am the head of GOP"

Two days later, another message from the GOP:

I am the head of GOP who made you worry. Removing Sony Pictures on earth is a very tiny work for our group which is a worldwide organization. And what we have done so far is only a small part of our further plan.It's your false if you if you think this crisis will be over after some time. All hope will leave you and Sony Pictures will collapse. This situation is only due to Sony Pictures. Sony Pictures is responsible for whatever the result is. Sony Pictues clings to what is good to nobody from the beginning. It's silly to expect in Sony Pictures to take off us. Sony Pictures makes only useless efforts. One beside you can be our member. Many things beyond imagination will happen at many places of the world. Our agents find themselves act in necessary places. Please sign your name to object the false of the company at the email address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger. Nobody can prevent us, but the only way is to follow our demand. If you want to prevent us, make your company behave wisely.

December 6th 2014 – "Gift of GOP for 2nd day"

GOP publish the following message:

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses. These are all confidential and include data related to sales plan of SPE. http://torrentproject.se/c8f4990114c6dc96af18f68f0c670a6e141298a6/ magnet:?xt=urn:btih:c8f4990114c6dc96af18f68f0c670a6e141298a6&dn=spe02&tr=http://retracker.perm.ertelecom.ru/announce&tr=udp://open.demonii.com:1337/announce&tr=udp://tracker.coppersurfer.tk:6969/announce Password: diespe123

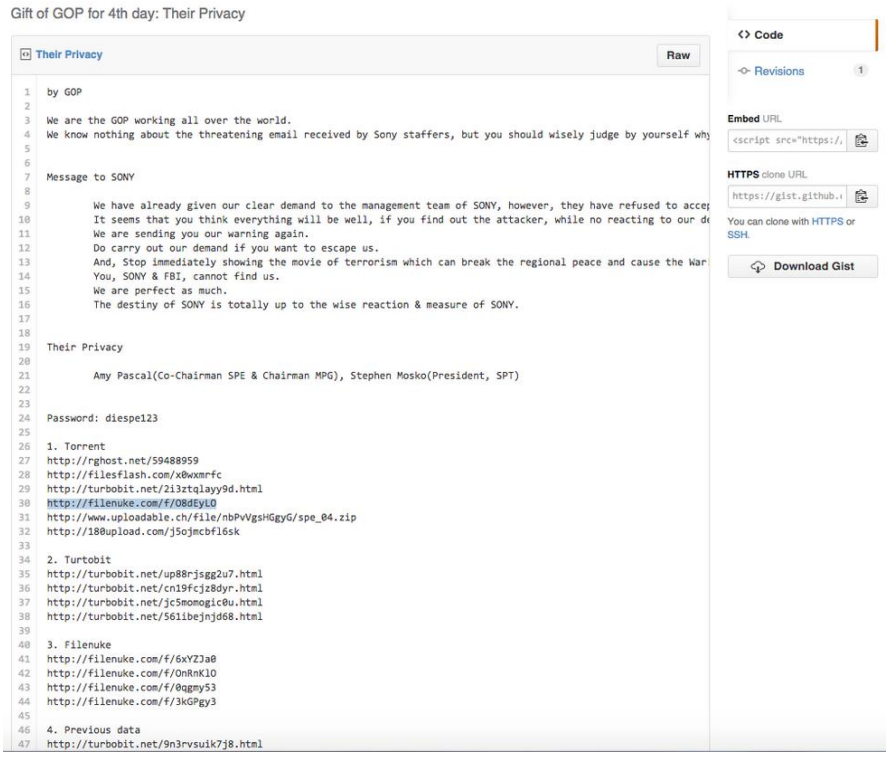
December 7th 2014 – "Gift of GOP for 3rd day Financial data of Sony Pictures"

GOP publishes the following message:

Anyone who loves peace can be our member. Please tell your mind at the email address below if you share our intention. Peace comes when you and I share one intention! 13 jack.nelson-63vrbu1@yopmail.com You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses. These include many pieces of confidential data. The data to be released next week will excite you more. Password: diespe123

December 8th 2014 – "Gift of GOP for 4th day"

GOP publishes a message targeting Sony executives:



Pic.16 – GOP announced that Sony refused to accept their "rules of the game"

December 10th 2014 – "Gift of Sony for 5th day: My Life At The Company-Part 1"

GOP publishes the following message:

To SPE employees. SPE employees! Don't believe what the executives of SPE says. They say as if the FBI could resolve everything. But the FBI cannot find us because we know everything about what's going on inside the FBI. We still have huge amount of sensitive information to be released including your personal details and mailboxes. If continued wrongdoings of the executives of SPE drive us to make an unwanted decision, only SPE should be blamed. Now is the time for you to choose what to do. We have already given much time for you.

December 11th 2014 - "Gift of Sony for 5th day: My Life At The Company-Part 2"

GOP publishes the following message:

by GOP
Important Message to SPE executives
I've sent you a message. Confirm your mailboxes.

The message is addressed from one person ("*I've sent you*"). After some time, another message was published:

We are preparing for you a Christmas gift. The gift will be larger quantities of data. And it will be more interesting. The gift will surely give you much more pleasure and put Sony Pictures into the worst state. Please send an email titled by "Merry Christmas" at the addresses below to tell us what you want in our Christmas gift.

December 14th 2014 - "The sooner SPE accept our demands, the better"

GOP released a new message to Sony, promising to bankrupt the company:

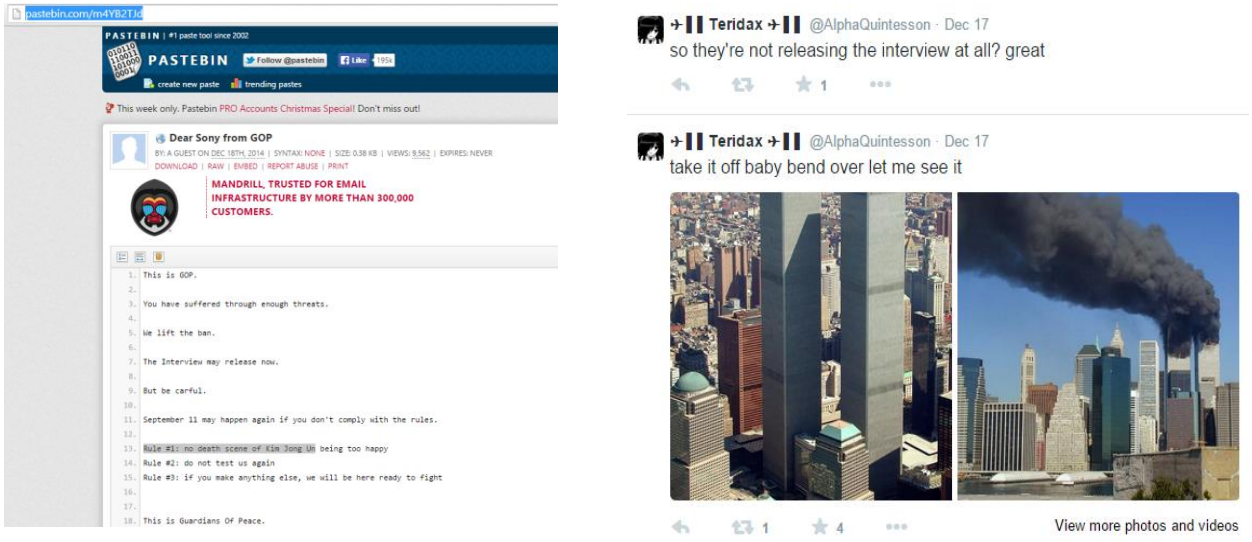
The sooner SPE accept our demands, the better, of course. The farther time goes by, the worse state SPE will be put into and we will have Sony go bankrupt in the end. Message to SPE Staffers. We have a plan to release emails and privacy of the Sony Pictures employees. If you don't want your privacy to be released [sic], tell us your name and business title to take off your data.

After the new leaked files were uploaded, former Lizard Squad member "Abdilo" posted:

"Sony could of avoided this if they would pay up the the extortion letter. Take this as a lesson companies, be prepared to loose everything."[10]
(December 17th, "Abdilo")

December 18th 2014 - "Dear Sony from GOP"

On December 18th, a published post on Pastebin from GOP[11], mentioning, "*September 11 may happen again if you don't comply with the rules*". The previous day, a Lizard Squad member actively discussed the 9/11 tragic incident in a satirical manner:

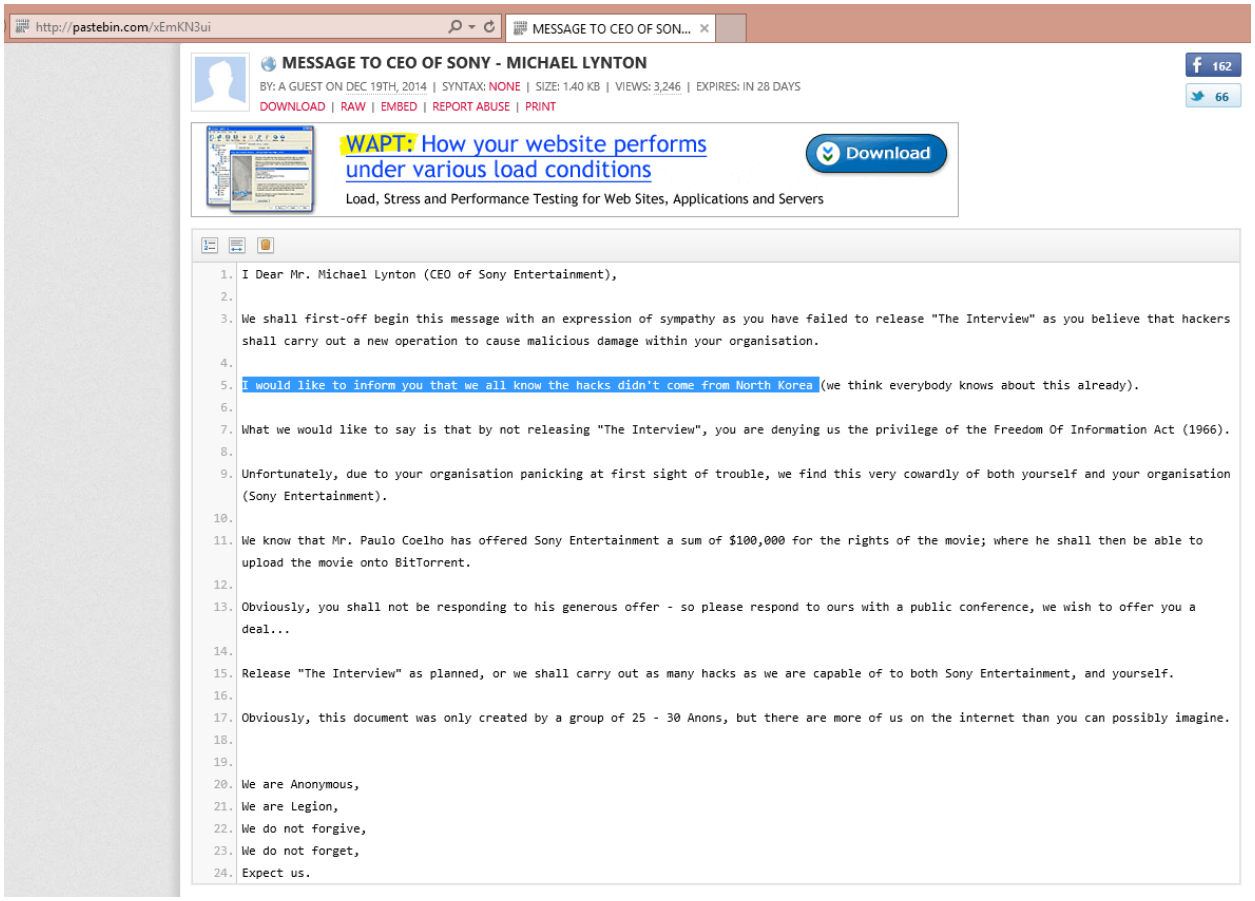


Pic.17 – Lizard Squad member and GOP mentioned the 9/11 incident in their postings

[10] https://twitter.com/abdilo_/status/545456086895960065
[11] http://pastebin.com/m4YB2TJd

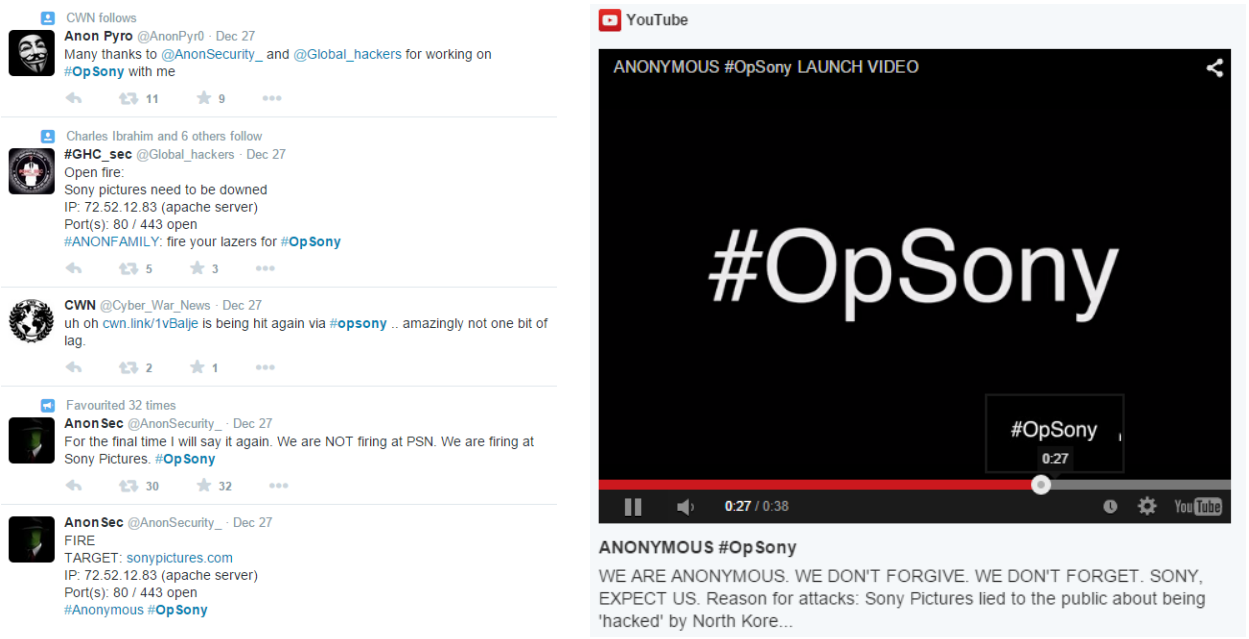
December 19th 2014 - "Message to CEO of Sony – Michael Lynton"

On December 19th there was a published post on Pastebin - http://pastebin.com/xEmKN3ui. The bad actors signed the message as "Anonymous" mentioning, "*We all know the hacks didn't come from North Korea*":



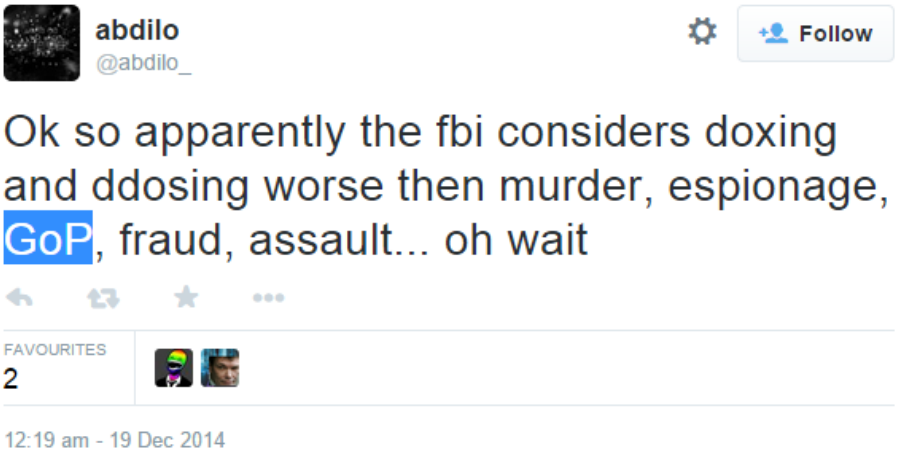
Pic.18 – One of the first messages to Sony from hackers with Anonymous signature

After this post, new independent Hacktivists appeared, with some participating and promoting "Anonymous" and starting #OpSony campaign.



Pic.19 – #OpSony will be targeted on DDoS against Sony Pictures

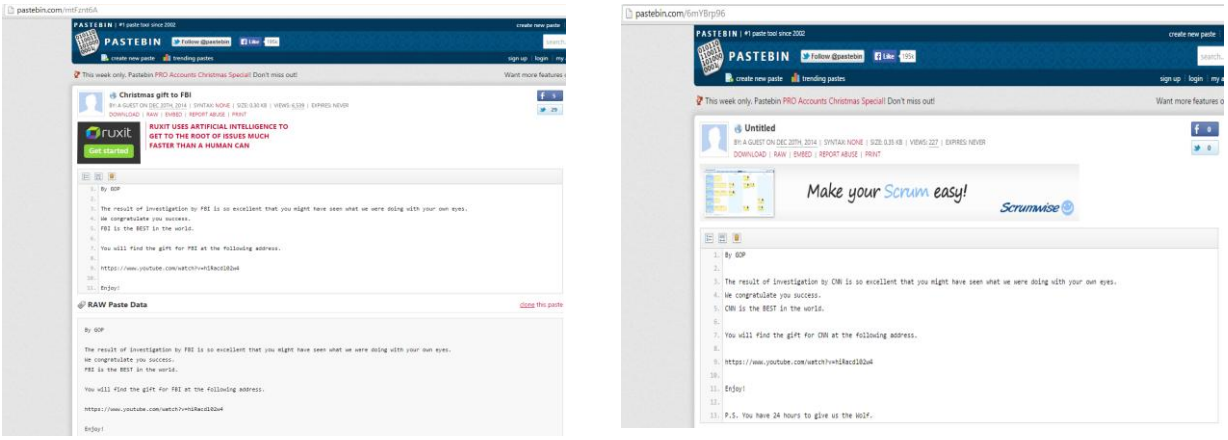
On the same day, former member of "Lizard Squad" mentions "GOP" and current investigation in satirical form:



Pic.20 – Former Lizard Squad member "Abdilo" mentioned GOP

December 20th 2014 - "Christmas gift to FBI"

After the new FBI update on the Sony hack[12], two published posts by GOP denied any link with North Korea:



Pic.21 – GOP will deny the link with North Korea in "Christmas gift" post

December 22th 2014 - "Working together with GOP on a Christmas project"

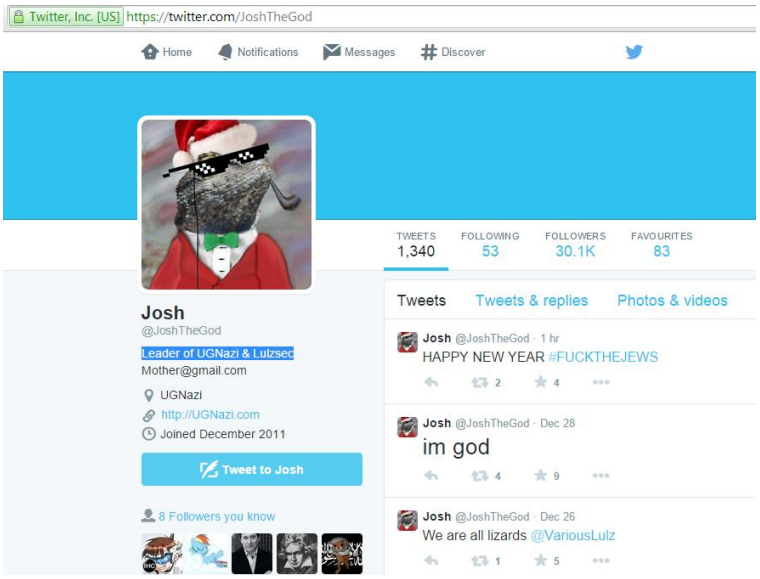
Lizard Squad published a post that they work with GOP[13] on a Christmas project:

[12] http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[13] https://twitter.com/LizardUnit/status/546752455661584385

Pic.22 – Lizard Squad announced work with GOP

An interesting fact is that the avatar of Lizard Squad is used by other hacking groups and their leaders, such as "JoshTheGod". This bad actor named himself as "Leader of UGNazi & LulzSec", groups that compromised Sony in 2011.



Pic.23 – Leader of UGNazi & LulzSec with the same avatar as Lizard Squad

Later, the Lizard Squad member, "Abdilo" explained that he left the group in October 2014, but retained relations with team members. Lizard Squad mentions GOP in some of their posts:

https://twitter.com/LizardMafia/status/547570060160954369
"greets from DPRK ;)==="

https://twitter.com/LizardMafia/status/547579229156954112
"We should do it too every channel. Greets to GoP & DPRK"

Pic.24 – Lizard Squad will greet GOP and DPRK (North Korea)

During active discussions of a possible film leak "The Interview", The Pirate Bay was defaced with picture of North Korea leader. "Abdilo" mentioned this incident with an ambiguous phrase: "GOP you trolls".

Pic.25 – "GOP you trolls" comment by Abdilo

December 29th 2014 - "Well, we do know some people from the GOP"

In an interview with the Washington Post[14], Lizard Squad explained, that they have links with "GOP" and provided the group with credentials for Sony hack:

Q: Some reports suggest you've got links to Guardians of Peace, and possibly to the Islamic State. Can you talk about that for a minute?

[Another long pause, about five minutes.]

A: Well, we do know some people from the GOP. We do not have any links to the IS.

Q: But you didn't work with Guardians of Peace to breach Sony's network and gain access to the e-mails, etc.? In other words, you know some people but weren't involved in the Sony hack surrounding 'The Interview'?

[A seven-minute pause.]

A: Well, we didn't play a large part in that.

Q: What part did you play?

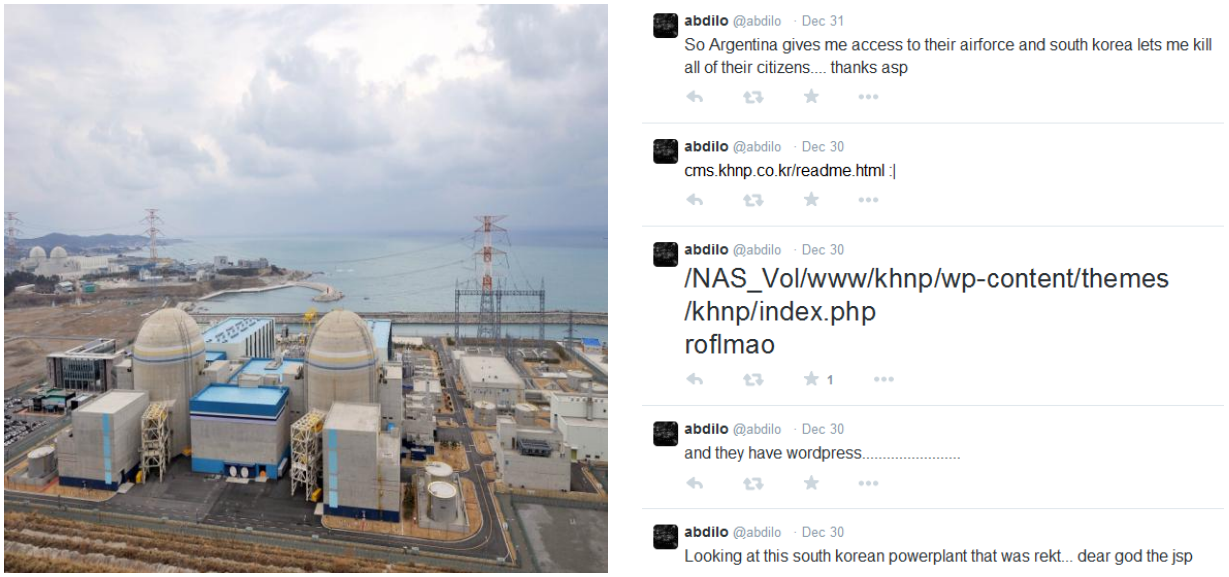
A: We handed over some Sony employee logins to them. For the initial hack.

December 30th 2014 - "Looking at this south korean powerplant"

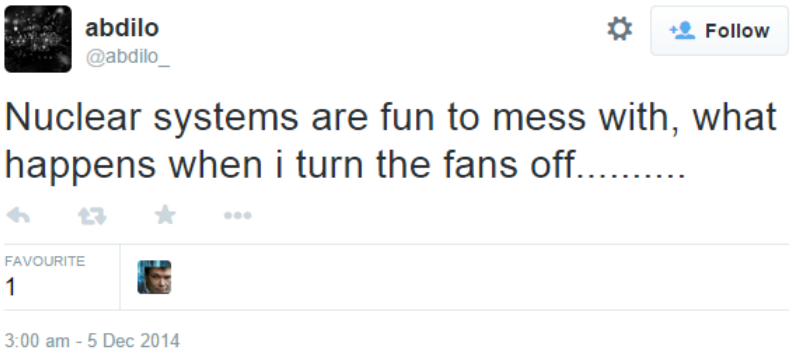
"Abdilo" has mentioned South Korean nuclear energy company KHNP, which was referenced in a Reuters article about a hacking attempt and leak of documents.

*Computer systems at South Korea's nuclear plant operator have been hacked, the company said on Monday, sharply raising concerns about safeguards around nuclear facilities in a country that remains technically at war with North Korea (**Reuters, December 22nd 2014**)*

[14] http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/29/a-qa-with-the-hackers-who-say-they-helped-break-in-to-sonys-network/



Pic.26 – Former Lizard Squad member "Abdilo" and vulnerabilities in KHNP



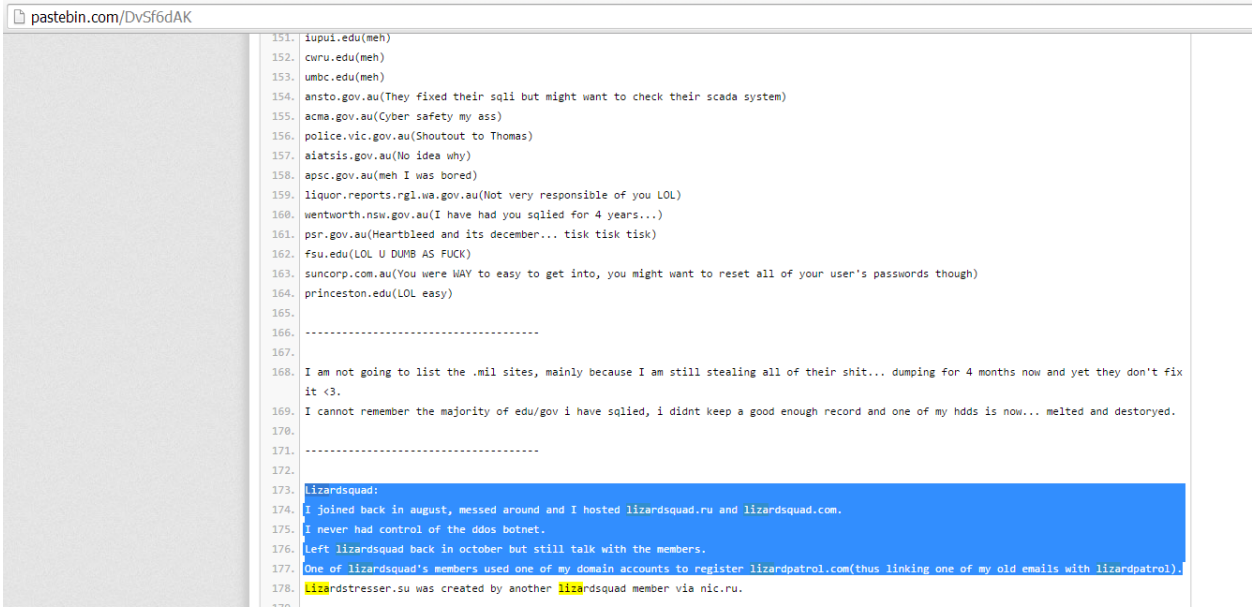
Pic.27 – The bad actor started his harmful activities in early December

December 31th 2014 - "Suicide Hacking in Australia"

The bad actor "Abdilo" published a very specific post on Pastebin about his past cyber attacks (URL: http://pastebin.com/DvSf6dAK).

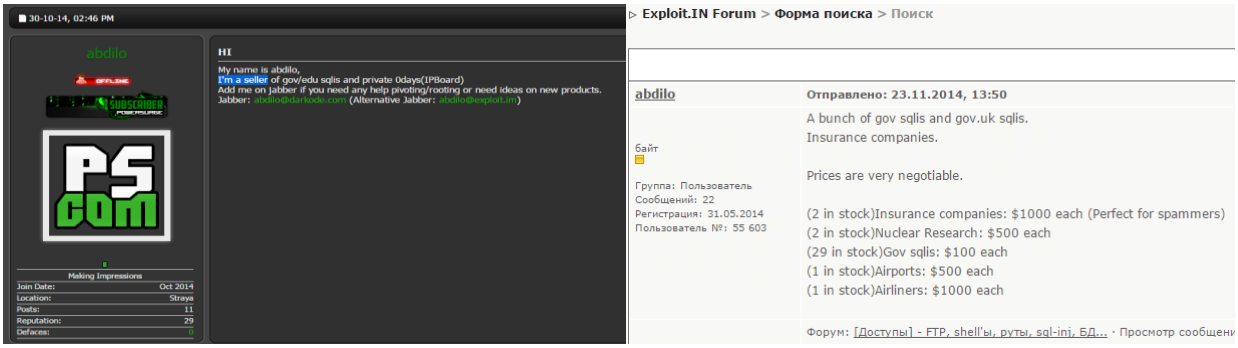
He enumerated some of his hacked targets in the past, and explained that he left Lizard Squad in October, but retained relations with its members.

*Now I am going to attack south korea... one uni now has no records, no mssql db, none of its asp/aspx and all external hdds have been formatted. (**31st December 2014, "Abdilo"**)*

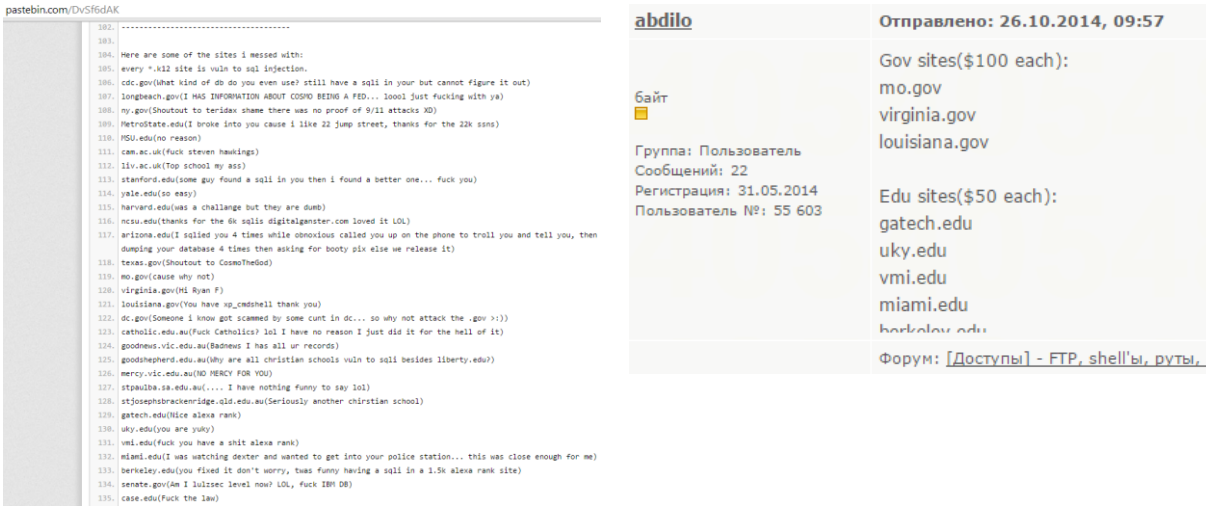


Pic.28 – Published list of hacked government resources by "Abdilo"

In October 2014, "Abdilo" started advertising his own services in the underground, related to the selling of vulnerabilities on government WEB-sites and private exploits.

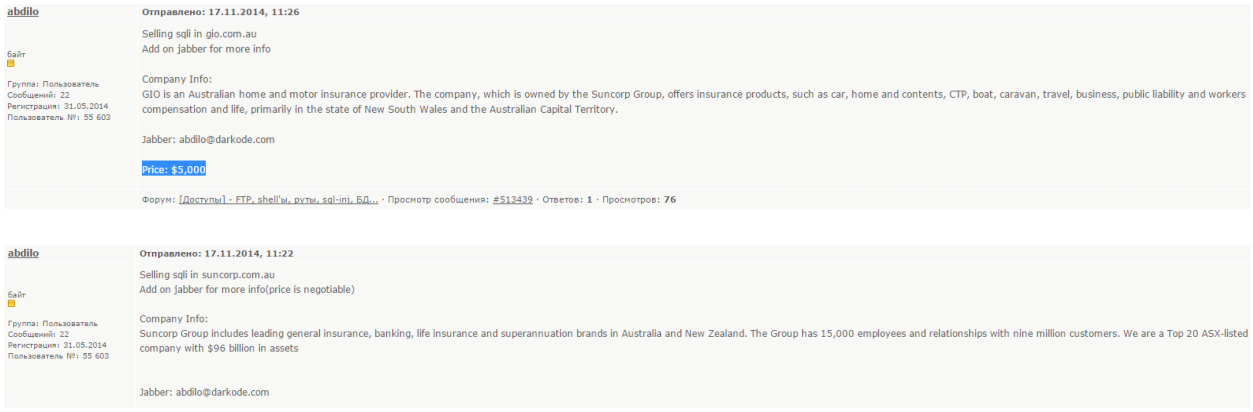


Pic.29 – "Abdilo" began advertising his own hacking services of .gov/.edu resources in the underground



Pic.30 – Published samples of compromised government resources

Besides government segment, he has also published for sale information about vulnerabilities in regard of leading insurance companies of Australia – SunCorp and GIO Insurance Australia.



abdilo

Отправлено: 17.11.2014, 11:26

Selling sqli in gio.com.au
Add on jabber for more info

байт

Группа: Пользователь
Сообщений: 22
Регистрация: 31.05.2014
Пользователь №: 55 603

Company Info:
GIO is an Australian home and motor insurance provider. The company, which is owned by the Suncorp Group, offers insurance products, such as car, home and contents, CTP, boat, caravan, travel, business, public liability and workers compensation and life, primarily in the state of New South Wales and the Australian Capital Territory.

Jabber: abdilo@darkode.com

Price: $5,000

Форум: [Доступы] - FTP, shell'ы, руты, sql-inj, БД... · Просмотр сообщения: #513439 · Ответов: 1 · Просмотров: 76

abdilo

Отправлено: 17.11.2014, 11:22

Selling sqli in suncorp.com.au
Add on jabber for more info(price is negotiable)

байт

Группа: Пользователь
Сообщений: 22
Регистрация: 31.05.2014
Пользователь №: 55 603

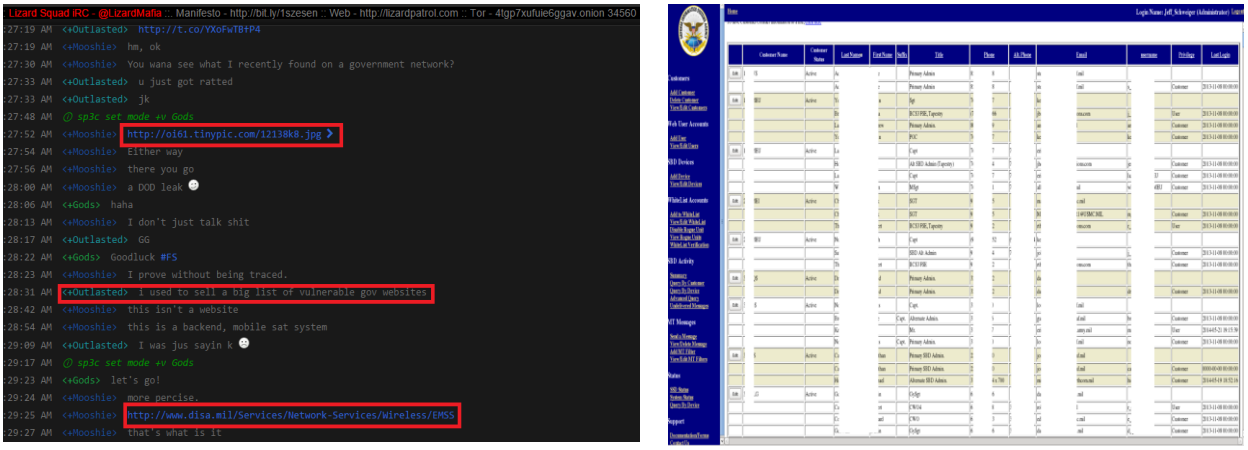
Company Info:
Suncorp Group includes leading general insurance, banking, life insurance and superannuation brands in Australia and New Zealand. The Group has 15,000 employees and relationships with nine million customers. We are a Top 20 ASX-listed company with $96 billion in assets

Jabber: abdilo@darkode.com

According to gathered information, he has compromised more than 60 government and educational WEB-resources, the majority of which were published in his posts[15].

I am not going to list the .mil sites, mainly because I am still stealing all of their shit... dumping for 4 months now and yet they don't fix it <3. I cannot remember the majority of edu/gov i have sqlied, i didnt keep a good enough record and one of my hdds is now... melted and destoryed.
(December 31th, "Abdilo")

During long term monitoring of the Lizard Squad IRC channel, several messages were identified referencing the hacking of military and government resources. This verifies that the objects of interests of the bad actors are not limited to gaming services only.



Lizard Squad IRC - @LizardMafia ::: Manifesto - http://bit.ly/1szesen :: Web - http://lizardpatrol.com :: Tor - 4tgp7xufuie6ggav.onion 34560

27:19 AM <+Outlasted> http://t.co/YXoFwTBfP4
27:19 AM <+Mooshie> hm, ok
27:30 AM <+Mooshie> You wana see what I recently found on a government network?
27:33 AM <+Outlasted> u just got ratted
27:33 AM <+Outlasted> jk
27:48 AM @ sp3c set mode +v Gods
27:52 AM <+Mooshie> http://oi61.tinypic.com/12138k8.jpg
27:54 AM <+Mooshie> Either way
27:56 AM <+Mooshie> there you go
28:00 AM <+Mooshie> a DOD leak
28:06 AM <+Gods> haha
28:13 AM <+Mooshie> I don't just talk shit
28:17 AM <+Outlasted> GG
28:22 AM <+Gods> Goodluck #FS
28:23 AM <+Mooshie> I prove without being traced.
28:31 AM <+Outlasted> i used to sell a big list of vulnerable gov websites
28:42 AM <+Mooshie> this isn't a website
28:54 AM <+Mooshie> this is a backend, mobile sat system
29:09 AM <+Outlasted> I was jus sayin k
29:17 AM @ sp3c set mode +v Gods
29:23 AM <+Gods> let's go!
29:24 AM <+Mooshie> more percise.
29:25 AM <+Mooshie> http://www.disa.mil/Services/Network-Services/Wireless/EMSS
29:27 AM <+Mooshie> that's what is it

Pic.31 – Analyzed communications from Lizard Squad channel and compromised military WEB-resources

[15] http://pastebin.com/DvSf6dAK

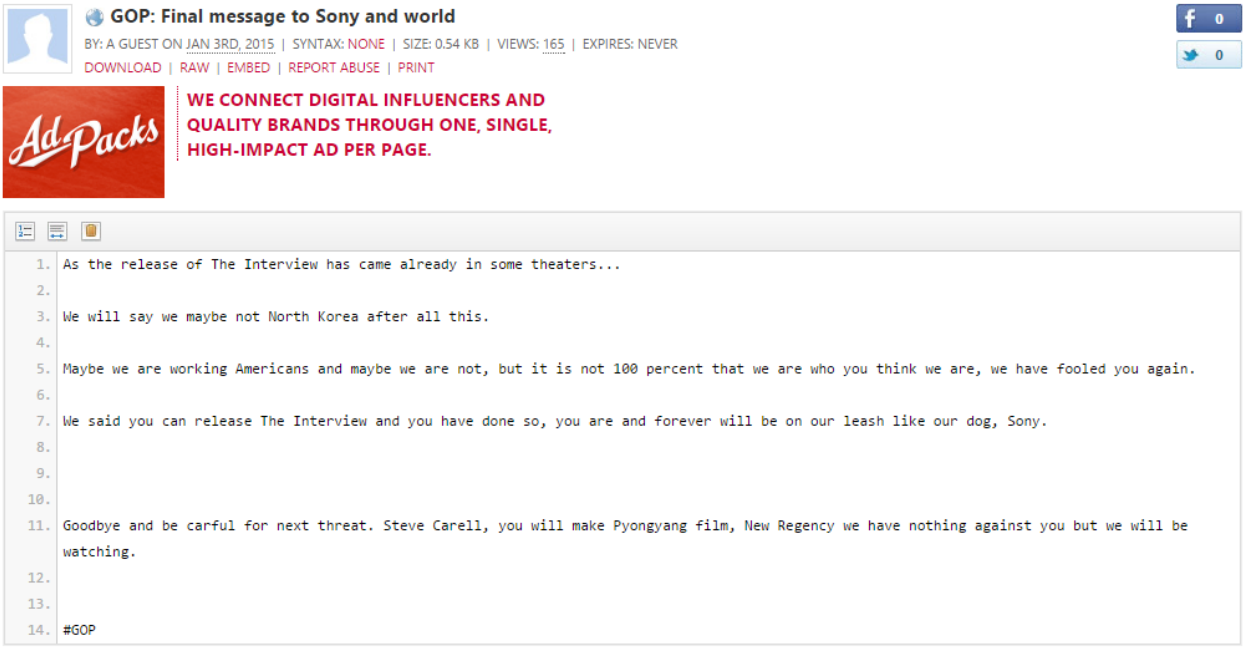
In his Twitter account, he mentions, that his future hacking activities will be targeted on South Korea - https://twitter.com/abdilo_/status/550466414897684483

Pic.32 – "Abdilo" will target his illegal activities against South Korea for reasons unknown

Provided facts may point at specifics surrounding the personal motivation of "Abdilo" and undisclosed customers of his services, who could use the results of his work for harmful activities.

January 3d 2015 - “GOP: Final message to Sony and world”

There was published anonymous post with the same style of text, signed by “GOP”[16].



Pic.33 – One of the latest messages, signed by GOP, after Sony hack

[16] http://pastebin.com/DZcSzy6N

Appendix A. - Lizard Squad / GOP Characteristics

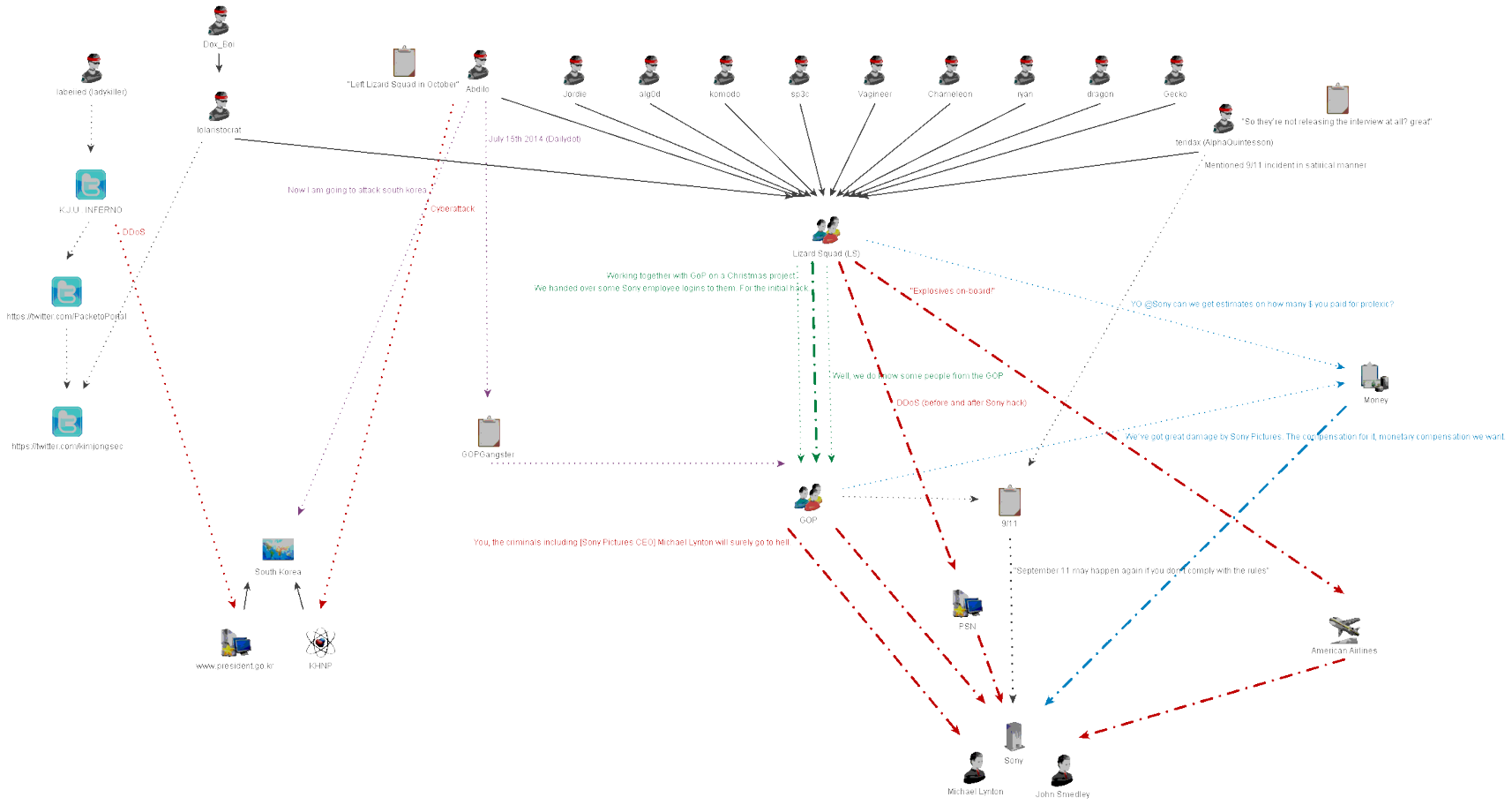
#	Lizard Squad	GOP
1	Lizard Squad has a leader, and group of hackers, performing cyber attacks.	GOP has a leader, calling himself "boss" or "head", coordinating other members.
2	Lizard Squad members are from the UK, Australia, Sweden and Finland, having fluent English.	GOP uses pretty good English in each of their messages to Sony, it doesn't have any incorrect translation and written in quite fluent form.
3	Lizard Squad member "Abdilo" has registered several domains in .RU, including official WEB-site of the group.	GOP used .RU server, besides others, where they have uploaded leaked files. Potentially, this server was compromised in the past.
	Lizard Squad member "Abdilo" left Lizard Squad in October 2014.	GOP released information about Sony in late November 2014.
4	Lizard Squad has threatened the victims with "*wonderful present to Christmas*". They also announced "*Working together with #GoP on a Christmas project*".	GOP has threatened Sony with "*Christmas gift*" too, which shows a correlation in timeline development and approach in dialogue with victims.
5	Lizard Squad member "Abdilo" has a GitHub account.	GOP has published several messages in GitHub, containing specifics.
6	Lizard Squad messages directly addressed to Sony several times, mentioning some commercial topics: *Sony, yet another large company, but they aren't spending the waves of cash they obtain on their customers' PSN server. End the greed.* *YO @Sony can we get estimates on how many $ you paid for prolexic?*	GOP messages addressed directly to Sony every time, including money compensation in order to prevent potential damage: *We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want.*
7	December 17th, Lizard Squad member "teridax" actively discussed 9/11 tragic incident in a satirical manner.	December 18th, GOP has published a post with phrase "*September 11 may happen again if you don't comply with the rules*".
8	Lizard Squad has words about North	GOP has mentioned the North Korean

	Korea at the end of their official song: "*North Korea…is the best Korea*"[17]	President in several of their posts. "*No death scene of Kim Jong Un being too happy*".
9	Sony was hacked by LulzSec in 2011. Lizard Squad affiliates have some members from other groups, such as "UGNazi" and "ex-LulzSec", using the same symbolic and style of posts. After the arrest of LulzSec members, the group was restructured.	So called "GOP" who compromised Sony in 2014, previously had no hacking activities or presence in the WEB.
10	Immediately after the Sony hack, Lizard Squad repeated DDoS attack on Sony PSN.	There is a correlation in harmful activities from Lizard Squad and GOP by time.
11	In an interview with the Washington Post, Lizard Squad explained, that they have links with "GOP" and provided them with credentials for the Sony hack. *Well, we do know some people from the gop.We handed over some Sony employee logins to them. For the initial hack.*	There is a correlation in harmful activities from Lizard Squad and GOP by means of attack, and by the fact, that one of Lizard Squad members "Abdilo" left the group in October 2014, before the Sony hack, which may show him as one of the potential bad actors, responsible for the new group GOP and past attacks.
12	In one of the articles, relating to the first DDoS attacks on big e-gaming services, there was a mentioned actor "GOPGangster". Lizard Squad member "Abdilo", using one of his old nicknames, commented the article.	There is a correlation between GOP as a group name, and links between Lizard Squad former member "Abdilo" and "GOPGangster".

. **Table 2** – Lizard Squad / GOP Characteristics Analysis

[17] https://www.youtube.com/watch?v=fS3cVh_vtsc

Appendix B. – Social Graph



Conclusion

Our analysis shows that young gamers were dissatisfied for a variety of reasons with the technology companies that provided them participating networks.

Attacking companies for fun, for a challenge, for a disliked policy, is really the ultimate online game. These identified bad actors seemed to have penetrated the networks over a substantial time period, giving them access to all types of intellectual property, corporate assets, and employee data. As discovered, these access points were offered up for sale or trade in the underground.

These groups are not solely restricted to the gaming sector but are clearly demonstrating their pursuit in other objects of interest.

The recent high profile targeted cyber attacks may have involved "for hire" hacker groups or independent Hacktivists.

Disclaimer

The research, findings, and analysis in this report are based on a combination of open and operative sources. To protect some victims and open cases, the non-disclosure of operative sources may leave some gaps in the linkage of some parts of the analysis. This report is solely the opinion of IntelCrawler LLC.

Trademarks
IntelCrawler, the IntelCrawler logo, and IntelCrawler's products and services are trademarks or registered trademarks of IntelCrawler LLC. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or the names of their products. IntelCrawler disclaims proprietary interest in the marks and names of others.